

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images,
Please do not report the images to the
Image Problem Mailbox.

Remarks

Claims 1-3, 5-20 and 22-27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jones (U.S. Patent No. 5,412,730) in view of Nardone et al. (U.S. Patent No. 5,805,700; hereinafter Nardone), and further in view of Leppek (U.S. Patent No. 5,933,501). Additionally, claims 1, 13, 14, and 26 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Aucsmith et al. (U.S. Patent No. 5,991,403; hereinafter, Aucsmith), in view of Nardone and Leppek; claims 4 and 21 are rejected under 35 U.S.C. §103(a) as being unpatentable over Jones, in view of Nardone and Leppek, and further in view of "Digital Television Archives Maturity" by Leonardo Chiariglione, copyrighted 1998 (Chiariglione '98); claim 28 was rejected under 35 U.S.C. §103(a) as being obvious over Warren et al. (U.S. Patent No. 5,719,937; hereinafter, Warren) in view of Nardone and further in view of Leppek; claims 29-30 and 32-38 were rejected under 35 U.S.C. §103(a) as being unpatentable over Jones in view of Warren, and further in view of Nardone and Leppek; and claim 31 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Jones, Nardone, Leppek and Chiariglione '98 in view of Warren. These rejections are respectfully, but most strenuously, traversed and reconsideration thereof is requested. Applicants respectfully submit that the final Office Action mischaracterizes the teachings of various ones of the applied patents in a hindsight attempt to reconstruct Applicants' claimed invention using Applicants' own disclosed subject matter. Applicants respectfully traverse the rejections since these mischaracterizations in the final Office Action void the underlying basis for the rejections.

An "obviousness" determination requires an evaluation of whether the prior art taken as a whole would suggest the claimed invention taken as a whole to one of ordinary skill in the art. In evaluating claimed subject matter as a whole, the Federal Circuit has expressly mandated that functional claim language be considered in evaluating a claim relative to the prior art. Applicants respectfully submit that the application of these standards to the independent claims presented herewith leads to the conclusion that the recited subject matter would not have been obvious to one of ordinary skill in the art based on the applied patents.

As recited in claim 1, for example, applicants' invention comprises a method for protecting a stream of data to be transferred between an encryption unit and a decryption unit.

The method includes encrypting the stream of data at the encryption unit for transferring of the encrypted stream of data from the encryption unit to the decryption unit. The encrypting of the stream of data is dynamically varied at the encryption unit by dynamically changing simultaneously multiple encryption parameters of the encryption process, and signaling the dynamic change in encryption parameters to the decryption unit. The dynamically varying of the multiple encryption parameters is responsive to occurrence of a predefined condition in the stream of data. Upon receipt of the encrypted data at the decryption unit, the method includes decrypting the encrypted data, wherein the decrypting accounts for the dynamic varying of the encrypting by the encryption unit using the simultaneously changed, multiple encryption parameters.

Advantageously, the present invention provides a new technique for protecting a stream of data to be transferred between an encryption unit and a decryption unit. The technique includes dynamically changing simultaneously multiple encryption parameters used to encrypt the stream of data as the stream of data is passing through the encryption unit. This dynamically changing can occur periodically over time, for example, several times a second, thereby allowing only a small segment of the stream of data to be decoded should the encryption parameters used to encrypt that segment of data be uncovered. This concept of dynamically changing simultaneously multiple encryption parameters as a stream of data is being encrypted is believed to comprise a unique approach from any of the applied art, which typically rely upon definition of a predefined policy for changing the encryption process.

Jones describes an encrypted data transmission system employing means for "randomly" altering the encryption keys. Pseudo-random number generators are employed at both the transmitting and receiving stations to supply identical sequences of encryption keys to a transmitting encoder and receiving decoder. An initial random number seed value is made available to both stations. The random number generators are advanced at times determined by predetermined characteristics of the data being transmitted so that, after transmission has taken place, the common encryption key can be known only to the transmitting and receiving stations.

A careful reading of Jones fails to uncover any teaching or suggestion of applicants' concept of encrypting a stream of data and during the encryption process dynamically varying

encrypting of the stream of data by dynamically changing simultaneously multiple encryption parameters. The Jones encryption approach requires pseudo-random binary sequence generation, and requires seed and mask values arranged at the sender and the receiver. Further, a change in Jones to the encryption process involves changing only an encryption key. The change in the encryption key occurs only at a predefined interval arranged a priori between the sender and the receiver. Jones changes the encryption key only when the counted number of bits or words or "items" matches the arranged interval. The disadvantage of this approach is that synchronization is absolutely essential. Bytes lost during transmission throw off the encryption/decryption process without any chance of recovery. In contrast, applicants' invention of dynamically varying simultaneously multiple encryption parameters as the stream of data is being encrypted ensures that only a small segment of the encrypted data could be exposed or lost should the encryption parameters used to encrypt that segment become uncovered or lost, respectively.

In addition, applicants' recited process includes signaling the dynamic change in the encryption parameters from the encryption unit to the decryption unit. A careful reading of Jones fails to uncover any teaching, suggestion or implication that the single encryption key change is signaled to the decryption unit. Rather, the patent teaches otherwise by describing a process which relies upon an a priori agreed upon process. In Jones, the decryption unit knows in advance where the encryption key change is to occur. In contrast, applicants recite a truly dynamic varying of the encryption process wherein the dynamically changed encryption keys are forwarded from the encryption unit to the decryption unit.

At page 35 of the final Office Action, the Examiner states that Applicants' recited aspect of "signaling the dynamic change in the encryption parameters from the encryption unit to the decryption unit" is taught by Jones at Col. 1, lines 66 to Col. 2, line 7, wherein there is an alleged exchange of random number seed values and interval values between the encryptor and decryptor. Applicants respectfully submit that these lines of Jones disclose an a priori arrangement whereby the seed values and interval values are made available to both the transmitting station and a receiving station. Fig. 1 of Jones clearly shows that the interval number and random number seed are inputs to both stations. The transmitting station does not forward the interval number and seed number to the receiving station. Thus, there is no dynamic signaling of information *per se* from the encryption unit to the decryption unit in Jones. In view

of this, Applicants respectfully submit that the final Office Action mischaracterizes the teachings of Jones when asserting those teachings against Applicants' invention as recited in the independent claims presented.

Nardone is cited in the final Office Action for allegedly teaching dynamically changing encryption parameters used to encrypt a stream of data (and presumably Applicants' recited concept of dynamically varying the encrypting of the stream by changing simultaneously multiple encryption parameters). This characterization of the teachings of Nardone are respectfully traversed.

Nardone describes a policy based selective encryption of compressed video data. Basic transfer units of compressed video data of a video image are selectively encrypted in Nardone in accordance with an encryption policy to degrade the video image to at least a virtually useless state, i.e., if the selectively encrypted compressed video image were to be rendered without decryption. A careful reading of Nardone fails to uncover any dynamic varying of the encryption parameters as a stream of data is being encrypted within an encryption unit as recited by applicants. The Office Action notes that Nardone teaches encrypting of a bit stream taking into account encryption granularity, density and delay. However, Nardone does not describe dynamically varying multiple ones of these encryption parameters simultaneously as the encryption of a stream of data progresses.

Nardone is characterized in the final Office Action as teaching specifying encryption parameters via a policy (i.e., the degree of selective encryption in order to degrade video image). This characterization of the teachings of Nardone is traversed. Nardone does not expressly describe varying of multiple encryption parameters, let alone simultaneously varying multiple encryption parameters dynamically during the encryption process. Nardone does teach multiple encryption policies can be provided at authoring time, and does discuss the possibility of changing between policies. However, Applicants respectfully submit that this change between policies merely results in a change in the duty cycle of the encryption process in Nardone, and does not depend upon or suggest that multiple encryption parameters are changed between the policies. A careful reading of Nardone fails to uncover any teaching or suggestion of such a concept. Notwithstanding this, the Office Action characterizes the change in encryption policy

(resulting in a change in the duty cycle in Nardone) as somehow equating to a dynamic change in multiple encryption parameters during the encryption process. Applicants respectfully submit that a change between predefined policies in Nardone does not equate to or suggest their recited process for dynamically varying the encrypting of a stream of data at an encryption unit by dynamically changing simultaneously multiple encryption parameters. The result of Nardone is simply a change in the duty cycle of the encryption process, and does not suggest that multiple encryption parameters are simultaneously varied during the encryption process. Thus, without hindsight reference to Applicants' claimed invention, it is respectfully submitted that one of ordinary skill in the art would not have read the teachings of Nardone as suggesting that multiple encryption parameters could be simultaneously varied dynamically during the encryption process.

Leppek is cited in the final Office Action for allegedly teaching setting multiple encryption parameters at once. This characterization of the teachings of Leppek is respectfully traversed.

Leppek describes a virtual encryption scheme which combines different encryption operators into a compound-encryption mechanism. The encryption operators in Leppek refer to different encryption processes. Thus, in Leppek, data is first encoded using a first encryption scheme, then the same data is encoded using a second encryption scheme, etc., thereby increasing the entropy of the data to make the encoded data look as random as possible.

In contrast, applicants recite dynamically changing simultaneously multiple encryption parameters while an encryption unit is encrypting a stream of data. In applicants' approach, different segments of the stream of data are encrypted using different encryption parameters and there is a dynamic change in the encryption parameters such that multiple encryption parameters simultaneously change from one segment to another segment of the stream of data as the stream of data is passing through the encryption unit and being encrypted. In Leppek, there is a static, sequential application of a number of encryption algorithms or encryption operators to the same segment of data. Leppek describes encrypting the same data multiple times using different encryption operators (i.e., encryption schemes).

At page 33 of the Office Action, the Examiner seeks to equate Leppek's teaching of a compound sequence of encryption operators, i.e., the sequential application of encryption algorithms, to Applicants' recited language of simultaneously changing multiple encryption parameters during the dynamically varying of the encrypting of the stream of data. The alleged insight of Leppek is application of multiple encryption operators at once. This conclusion is respectfully traversed. Leppek does not teach the application of multiple encryption operators being applied to the data simultaneously. Rather, Leppek describes a sequential application of encryption algorithms to the same data to increase the entropy of the data. Since Leppek describes a process of sequentially applying different encryption processes to the same data, Applicants respectfully submit that the insight allegedly drawn therefrom is in error.

Additionally, Applicants respectfully submit that one of ordinary skill in the art would not have combined Jones, Nardone and Leppek as proposed in the final Office Action. For example, Jones relies on a fixed policy or fixed sequence for changing a single encryption parameter. Nardone describes a process for varying the duty cycle of an encryption scheme based on predefined policies, and Leppek describes a virtual encryption scheme which combines different encryption processes into a sequential, compound encryption mechanism. None of these references, taken singularly or in combination, suggest Applicants' recited concept of dynamically changing the encryption process by simultaneously changing multiple encryption parameters as a stream of data is being encrypted. Because Applicants' approach does not rely upon any predefined policy, the dynamic change in the multiple encryption parameter is signaled from the encryption unit to the decryption unit. Jones, Nardone, and Leppek do not describe any mechanism for signaling dynamic changes in multiple parameters from an encryption unit to a decryption unit. In this regard, Jones does not describe signaling of encryption parameter changes from the encryption unit to the decryption unit. In Jones, a seed value and interval value are established a priori before an encryption process begins and are provided as inputs to both the encryption unit and the decryption unit (see Fig. 1 of Jones). Since they are provided a priori as inputs to both units, there is no signaling from the encryption unit to the decryption unit of the simultaneous change of multiple encryption parameters.

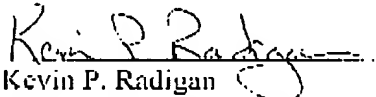
For the above reasons, Applicants respectfully request reconsideration and allowance of independent claims 1, 14 & 27. Claims 1 & 14 are also believed allowable over the combination of Auesmith, Nardone and Leppek stated in the final Office Action. The teachings of Auesmith are similar to those of Jones when applied against the independent claims presented, and are believed distinguishable for the reasons stated above in connection with Jones. As noted in the final Office Action, Auesmith teaches generation of an encryption key for each Group Of Pictures (GOP) in a stream of video data. For each GOP, an encryption transformation, parameterized by the encryption key of the GOP, is applied to pictures of the GOP. Applicants respectfully submit that Auesmith teaches an approach for changing a single encryption parameter between GOPs, and is therefore analogous to the teachings of Jones described above when applied against Applicants' independent claims. Thus, for the reasons stated above, Applicants respectfully request reconsideration and withdrawal of the rejection to independent claims 1 & 14 based upon the combination of Auesmith, Nardone and Leppek.

Similarly, the rejection to independent claim 28 based upon Warren in view of Nardone and Leppek is respectfully traversed for the reasons stated herein above with respect to Jones, Nardone and Leppek. Warren describes an encryption process using a scheme such as Hidden Data Transport (HDT) and Post-Compression Hidden Data Transport (PC-HDT). Warren describes certain advantages of using HDT and PC-HDT algorithms over other encoding technologies, but does not even describe switching between HDT and PC-HDT algorithms dynamically. Thus, Applicants respectfully submit that Warren is less relevant to their claimed invention than the Jones patent described above. Thus, for the above stated reasons, Applicants respectfully request reconsideration and withdrawal of the obviousness rejection to independent claim 28.

The dependent claims are believed allowable for the same reasons that the independent claims from which they directly or ultimately depend, as well as for their own additional characterizations. Chiariglione '98 is not believed to teach or suggest any of the above-noted deficiencies of Jones, Nardone, Leppek, Auesmith or Warren when applied against the independent claims presented herewith.

All pending claims are believed to be in condition for allowance and such action is respectfully requested. Should the Examiner wish to discuss this case with Applicants' attorney, the Examiner is invited to contact Applicants' representative at the below-listed number.

Respectfully submitted,


Kevin P. Radigan
Attorney for Applicants
Registration No.: 31,789

Dated: May 17, 2004.

HESLIN ROTHENBERG FARLEY & MESITI P.C.
5 Columbia Circle
Albany, New York 12203-5160
Telephone: (518) 452-5600
Facsimile: (518) 452-5579